情 報 保 護 學 會 誌
第 14 券 第 5 號, 2004. 10

서비스 현실화에 중점을 둔 인터넷 전자 투표 시스템

이 래*, 이 동 훈**

요 약

현재까지 전자투표 프로토콜이 다수 제안되었으나, 선거관리자의 부정 투표, 부정 개표를 투표자 입장에서 막거나 예방할 수 있는 장치들이 부족했다. 이러한 문제들을 단순히 가정(assumption)으로 단정한 후 설계된 프로토콜들은 현실적으로 적용하기에 큰 어려움이 따른다. 어떤 시스템이든 실질적인 서비스가 가능하도록 설계되기 위해서는 현실적인 가정에 근거해야 한다. 본 논문에서 제안하는 시스템은 비현실적인 가정에 의존하지 않고 투표서버와 개표서버의 부정행위를 사전에 예방할 수 있다. 또, 기존 암호 라이브러리를 그대로 사용할 수 있고 국내 PKI와의 연동이 쉬워 "주민투표제"와 전자정부 성격에 부합되는 시스템이다. ElGamal암호 알고리즘, Schnorr 은닉암호와 같이 연산량을 많이 요구하고 암호문이 기하급수적으로 증가되는 알고리즘을 사용하지 않아 계산적으로도 효율적이며, 투표자가 개표결과에 자신의 투표 내용이 올바르게 반영되었는지 확인할 수 있는 안전한 전자투표 시스템이다.

Ⅰ. 서 론

오늘날 컴퓨터와 네트워크 기술의 발전은 인간이 과거에는 상상하지 못하던 많은 일들을 가능하게 하고 있다. 전자 투표는 기존 오프라인에서의 투표와 달리 투표의 모든 과정이 인터넷을 통해 이뤄지는 것을 말한다. 유권자는 투표를 위해 투표소를 방문할 필요가 없고 인터넷을 사용할 수 있는 공간 어디에서나 투표에 참여할 수 있어 편리하다. 장애인처럼 선거참여가 쉽지 않았던 사람들도 쉽게 투표권을 행사할 수 있으며, 선거비용도 대폭 감소시킬 수 있다. 하지만, 이러한 장점들을 가진 전자투표가 우리 사회의 민주주의에 큰 도구로 이용되기 위해서는 어떤 불법적 개입에 대해서도 안전한 전자투표시스템이 필요하다. 많은 사람들이 참여하는 전자투표가 특정 공격에 취약하다면 사회적으로 큰 혼란을 불러 올 수 있다. 그러므로 전자투표는 가장 높은 수준의 암호학적 안전성을 요구하게 된다.

본 논문에서는 공개키 암호를 이용하여 투표 내용의 기밀성과 투표자의 익명성을 보장하면서도 투표자가 직접 자신의 의견이 투표결과에 반영되었는지 검증 가능한 안전한 인터넷 전자투표 시스템을 제안한다. 그리고 이러한 시스템을 실제 운용하여 서비스하기 위해서는 어떠한 부가적인 장치들이 필요한지 알아보겠다.

Ⅱ. 전자투표의 요구사항

전자투표는 투표와 관련된 일련의 과정들이 공정하고 안전하게 유지되도록 암호기법을 사용해서 이뤄진다. 이러한 전자투표 시스템이 갖춰야할 요구사항으로는 다음과 같이 7가지가 있다.[1]

- ⊙ 완전성(Completeness) : 모든 정당한 유효 투표는 정확하게 투표 결과에 집계되어야 한다.
- ⊙ 건전성(Soundness) : 부정 투표자에 의하여 투표가 방해되어서는 안 되며, 투표 결과에 부정 투표가 집계되어서도 안 된다.
- ⊙ 기밀성, 익명성(Privacy) : 모든 투표는 비밀리에 이뤄져야하며, 투표자의 투표내용을 알 수 없어야 한다.
- ⊙ 이중투표불가성(Unreusability) : 정당한 투표자는 두 번이상의 투표를 할 수 없어야한다.
- ⊙ 권한성(Eligibility) : 투표권이 없는 사람은 투표에 참여 할 수 없어야 한다.
- ⊙ 공정성(Fairness) : 투표에 영향을 미치는 일이 없

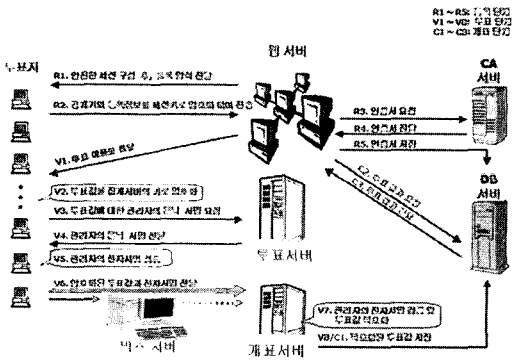
* 국가보안기술연구소 (raedit@etri.re.kr)
** 고려대학교 정보보호대학원 (donghlee@korea.ac.kr)

어야한다. 특히, 투표과정 중 일부분의 투표내용이 알려져 투표에 영향을 미쳐서는 안 된다.

⊙ 검증성(Verifiability) : 투표결과를 조작할 수 없도록 누구라도 자신의 투표내용이 투표결과에 반영되었는지 검증할 수 있어야 한다.

Ⅲ. 관련 연구

homomorphic encryption, mix-net, 은닉 서명 등 여러 가지 암호학적 기법을 통해 고안된 전자투표 프로토콜들이 많이 있다. 하지만, 전자투표 요구사항들을 모두 만족하더라도 많은 수의 투표자에 대하여 계산적, 저장 공간적으로 효율적이고 현실에 적용하여 구현 가능한 프로토콜은 많지 않다. 공개키 암호 알고리즘을 기반으로 설계된 전자투표 프로토콜로 은닉 서명과 bit-commitment를 이용한 1992년의 "A Practical Secret Voting Scheme for Large Scale Election"[2]가 있다. 하지만, 투표자가 개표 시에 다시 모두 참여해야한다는 문제점을 가지고 있다. 이러한 단점을 현실적으로 수정한 것이 1999년 제안된 "An Improvement on a Practical Secret Voting Scheme"[3][4]와 이와 유사한 "공개키 기반 구조 하에서의 안전한 인터넷 전자투표 프로토콜"[5][6]이다. 이들은 Elgamal 암호화 기법을 응용한 은닉서명과 threshold 암호기법을 사용해 고안된 것이다. 하지만, 이산대수문제에 기반한 은닉서명[7]을 사용했기 때문에 지수승 계산이 증가되는 단점이 있다. 특히 하나의 평문에 대해 암호문이 두개로 증가하는 Elgamal 암호와 DSA를 사용할 경우에는 투표자와 선거, 개표, 혼합서버(Mix Server) 간에 전송되는 메시지 양이 기하급수적으로 증가하기 때문에 매우 비효율적이다. 투표자와 투표내용에 대한 연계정보를 감추기 위해 혼합서버를 따로 사용하기 때문에 메시지 전송 횟수와 암복호화 횟수를 더 증가시키는 요인이 된다.



〔그림 1〕 일반적인 PKI기반의 전자투표 시스템

이제까지 연구된 전자투표 프로토콜들의 또 다른 문제점은 투표서버를 신뢰해야한다는 가정이 필요하다는 것이다. 하지만, 이것은 매우 비현실적인 가정이며, 전자투표가 실용화되지 못하는 큰 이유 중의 하나이기도 하다. "투표서버를 신뢰한다."라는 가정을 다르게 말하면, "투표서버가 임의로 올바른 유권자의 표를 대신하여 자신이 만든 임의의 부정 투표를 삽입할 수도 있다"는 것이기 때문이다.

Ⅳ. 서비스 현실화를 고려한 주요 개선 사항

본 논문에서는 기존의 전자투표 프로토콜의 단점을 개선하면서 우리나라 공개키 기반구조의 성격에 부합되도록 현실 적용의 관점에서 설계하는데 중점을 두었다. 비용 측면, 신뢰성과 안전성 측면에서 주요 개선 사항들을 정리하면 다음과 같다.

1. 현실적인 최소한의 가정

Honest Verifier, Honest Randomizer와 같은 가상의 증명자나, 투표자와 선관위의 도청 불가능한 안전한 채널 등의 기존 다른 전자 투표 프로토콜들이 지니는 현실세계에 적용하기 어려운 가정(Assumption)들을 배제하고 가장 현실적이고 최소한의 가정인 "투표서버와 개표서버간의 담합이 존재하지 않아야 한다."라는 것에만 의존한다.

2. 유권자의 투표 결과 검증 기능

유권자의 투표 과정을 간편화 시키면서도 개표 결과에 대한 검증 자료를 개표 결과 공고 시 함께 공개하여 유권자 스스로 자신의 투표 내용이 개표 결과에 올바르게 반영되었는지 확인할 수 있어 개표 결과에 대해 신뢰할 수 있다. 물론 타인의 투표 내용을 알 수는 없게 한다.

3. 투표함 혼합 서버(MIX Server) 제거

투표자와 투표내용간의 연관성을 제거시키는 Mix Server의 기능을 투표서버와 개표서버에 분산시켜 암복호화, 서명 및 검증 연산을 줄인다. 그리고 이를 통하여 Mix Server 운영에 필요한 하드웨어 또는 소프트웨어 비용을 절감시키고 Mix Server에 대한 DDOS공격이나 해킹 등의 시스템 공격에 노출되지 않도록 한다.

4. 다양한 공개키 암호 알고리즘 적용

지수승 계산을 많이 요구하고 암호문이 2배로 증가되는 ElGamal 암호 알고리즘에 의존하지 않도록 하고, 더 나아가 특정 공개키 암호 알고리즘에 의존하지 않고 RSA, ECC 등의 여러 가지 공개키 암호 알고리즘에 대한 적용이 가능하도록 한다. 특히, 기존 국내 PKI 인증서에서 사용하고 있는 암호 키를 그대로 사용할 수 있도록 하여, 국내 PKI와의 연동이 쉽고, 별도의 인증 체계 시스템이 필요 없도록 한다. 이는 암호학적 라이브러리와 같은 기존의 각종 기반 구조(Infrastructure)를 그대로 사용할 수 있으며, 결국 많은 비용을 절감할 수 있도록 한다.

5. 시스템 확장성

공개키 기반 구조가 갖춰지지 않는 환경이라 하더라도 전자투표 시스템 구축이 가능하도록 한다. 즉, 공인인증서를 활용하지 않는 환경이라면 시스템의 큰 변경 없이도 패스워드를 사용하여 투표자 인증 과정을 대체할 수 있도록 한다.

6. "주민투표제"와 전자정부 성격에 부합되는 투개표 구조

공개키 기반 구조(PKI)에 입각하여 설계하여 주민 개개인에게 주어진 인증서를 통해 인증 및 투표에 활용 할 수 있도록 하고, 찬반 혹은 양자택일의 주민 투표제에서도 투표내용의 비밀성과 투표자의 익명성이 유지될 수 있도록 한다. 뿐만아니라 의도적으로 무효표를 발생시킬 수 있는 오프라인의 투표방식의 여러 특징을 그대로 온라인에서도 구현한다. 투표에 소요되는 서버는 투표서버와 개표서버로 단 두 개의 서버만 존재하도록 하여, 단체장, 의회, 시민단체의 추천으로 구성되는 9인의 "주민투표관리위원회"에서 융통성있고, 서로 담합하지 못하도록 운영체계를 갖출 수 있게 한다. 이를 통해 전자투표의 활용도와 신뢰도를 높이도록 한다.

7. 투표자의 투표사실 부인봉쇄

기존 전자투표 프로토콜들의 경우는 투표자가 자신이 유효하게 투표를 마쳤음에도 불구하고 이의를 제기했을 경우 선관위에서 투표자의 투표사실을 입증할 증거가 부족했으나, 본 프로토콜의 경우는 이런 단점을 보완하여 투표가 완료되면서 투표자는 투표종료의 확인으로 자신만이 알고 있는 특정 비밀정보를 공개하고 이를 통해 자신의 투표 사실에 대한 부인을 못하게 한다. 이것은 전자투표라는 특수한 경우에만 가능한 것으로 1인 1투표제라는 특성을 활용한 것이다.

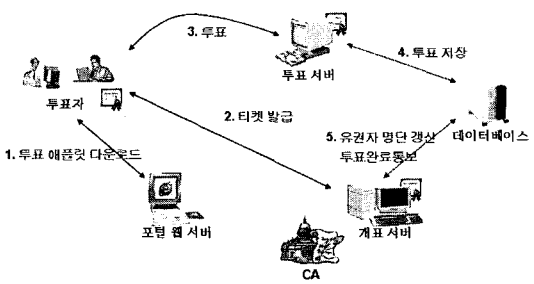
8. 전자투표 단말기가 설치된 투표소에서도 가능한 전자투표 시스템

궁극적으로는 인터넷 환경에서 가능한 시스템이지만 단계적으로 적용 가능성을 시험하기 위하여 소규모 회의상에서도 실현 가능하며, 또한 전자 투표 단말기가 설치된 투표소 환경에서도 가능하도록 한다. 이러한 단계적인 적용 시험을 통하여 계속적으로 시스템에 대한 신뢰성을 확보하고, 서비스의 안전성을 꾀할 수 있을 것이다.

V. 제안하는 인터넷 전자 투표 시스템

본 논문에서 제안하는 전자투표 시스템은 공개키 기반 구조(PKI)가 구축되어있는 환경에서 공인인증서를 활용하여 유권자 인증을 하는 경우와 PKI 환경이 구축되어있지 않아도 패스워드 등록방식을 통해 유권자 인증을 하는 경우 두 가지로 사용 할 수 있다. 기본적인 프로토콜의 내용은 PKI가 구축되어있는 환경에서의 전자투표 시스템 운용 및 유권자 서비스 절차를 설명하겠다. PKI가 구축되어 있지 않은 경우도 이와 크게 차이는 없고, 유권자 인증과정과 사전 등록 단계에 있어서 약간의 수정만 있으면 된다. 본 전자투표 시스템의 경우 크게 세가지의 단계로 구성되는데, 사전 등록 단계, 투표단계, 개표단계가 그것이다.

사전 등록 단계에서는 먼저 선거관리위원회에서 유권자 명단을 확정하고 이 유권자 명단을 데이터베이스로 만든 후 이에 대한 접근 권한을 투표 서버와 개표서버에게 모두 할당한다. 단, 유권자 명단에 대한 접근은 두 서버가 모두 가능하나 해당 필드별로 쓰기 권한은 다르게 부



〔그림 2〕 제안하는 전자투표 시스템의 기본 구성

여한다. 투표서버는 투표과정에서 투표함 데이터베이스를 비밀스럽게 유지하고 투표가 완료되면 투표함을 섞은 후 개표서버에게 접근 권한을 이양한다. 즉, 투표함을 옮겨 주는 것이다. 그리고 개표 서버는 투표함을 다시 섞은 후 개표 집계를 하게 된다. 그러면 먼저 전자투표 시스템의 주요 참여 개체(Entity)에 대해 설명하고, PKI 환경이 구축되어 공인인증기관과 공인인증서를 활용 할 수 있는 환경에서의 전자 투표 시스템의 세부 프로토콜부터 설명하겠다.

1. 전자 투표 시스템의 주요 개체(Entity)

o 투표자(클라이언트) : 안건에 대해 정당한 투표권을 가진 투표자(유권자). 인터넷에 접속 가능한 장비를 이용해 투표 서버에 접속하여 투표 수행.

o 선거 관리 위원회 : 선거와 관련된 제반 여건을 마련하고 관리 감독하는 기구. 투표내용을 공고하고, 투표 일정을 관리하며, 유권자 명단을 작성. 투표일 기준으로 개인의 투표권 여부를 판단하여 그 결과를 개인들에게 알리고 투표 참여를 유도.

o 투표 관리 위원회 (투표서버) : 투표 개시 후 투표 작업, 투표함 관리를 담당하는 기구. 투표 시 투표하려는 자의 투표권 여부, 이중투표 여부를 확인. 투표 시 정당한 투표자가 투표함에 자신의 투표가 올바르게 이뤄질 수 있도록 관리.

o 개표 관리 위원회 (개표서버) : 투표 마감 후 투표함에 대한 개표(투표 결과 집계)를 담당. 투표 중 투표 관리 위원회가 임의의 가짜 투표를 못하도록 감시. 투표 관리 위원회로부터 투표함을 넘겨받은 후 개표 작업 시행. 개표 결과와 개표 결과 검증 자료를 공개, 투표자들이 자신의 투표 결과를 확인토록 함.

2. PKI가 구축되어 공인인증기관과 공인인증서를 활용할 수 있는 환경에서의 전자투표 시스템

2.1 사용되는 자료구조(DataBase)

o 투표자 명단 (UserDB)

필드 명	내 용	쓰기 권한 (읽기는 모두 가능)	
		투표서버	개표서버
ID	주민등록번호	●	
Name	성명	●	
CA	인증서 발급기관	●	

o 투표자 명단 (UserDB)〈계속〉

필드 명	내 용	쓰기 권한 (읽기는 모두 가능)	
		투표서버	개표서버
Serial	인증서 일련번호	●	
Certificate	인증서	●	
Timestamp	투표 시간	●	
Vote IP	투표에 사용된 IP	●	
VC	투표자의 투표종료확인 서명	●	
EC	투표자의 투표종료확인 code		●

o 투표함 (VoteDB)

필드 명	내 용
number	투표함을 섞을 때 사용되는 숫자 (random sort sequence)
xi	개표서버의 공개키로 암호화된 투표 값
yi	xi에 대한 투표관리위원회의 서명 값
Valid	yi에 대한 서명 검증 결과

2.2 기호 정의

o VN : 전체 유권자 수

o A : 투표 관리 위원회(투표 서버)

o C : 개표 관리 위원회(개표 서버)

o Vi : i번째 투표자

o Ti : i번째 티켓

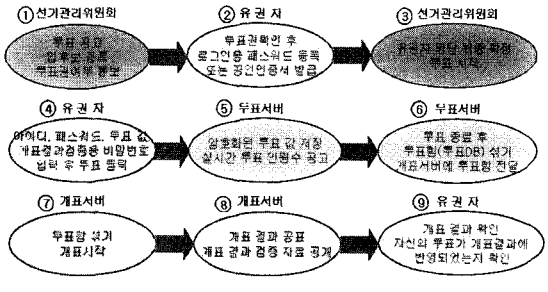
o Ts : 타임스탬프(Timestamp)

o ViC_key : i 번째 투표자와 개표관리위원회간의 대칭키 암호통신을 위한 대칭암호 비밀 세션 키

o xor : 비트간의 Exclusive-OR 연산

o v : 투표자가 선택한 투표값

o r : 투표자가 개표결과 검증을 위해 선택한 자신만이 알고 있는 비밀번호(숫자 8자리)



〔그림 3〕 인터넷 전자투표 시스템의 개괄적인 절차

o Hash() : 일방향 해쉬 함수
o Sign(), Verify() : 전자 서명 / 검증 함수
o SE() : 비밀키(대칭키) 암복호화 알고리즘

2.3 전자 투표 세부 과정

o 투표사전단계

(1) 선거관리위원회에서는 해당 선거 또는 투표의 내용을 공지하고 적정 기준에 의거하여 유권자를 선별하고, 유권자 개인들에게 투표권 여부를 우편, 전화, 이메일 등의 방법으로 통보한다.
(2) 유권자들은 자신의 투표권 여부를 선거관리위원회의 공개게시판에서도 확인할 수 있으며 투표권에 대한 이의를 제기할 수 있다.
(3) 투표권을 가진 유권자는 자신이 공인인증서를 소유하고 있는지 확인하고, 없을 경우 자신의 비밀키와 공개키를 생성하고 이를 이용하여 공인인증기관을 통해 인증서를 발급받는다. 공인인증서 발급과 관련한 사항은 "전자서명법"과 공인인증기관의 인증업무준칙 등에 명시된 바에 따른다.
(4) 선거관리위원회는 일정시간까지 유권자의 투표권 이의제기를 받고 이를 확인 조정한 후, 유권자 명단을 완성한다. 즉, 투표자 명단 Database인 UserDB의 ID, Name을 기재하고 최종 유권자 명단을 확정한다. 그리고 USERDB에 대한 접근 권한을 투표관리위원회와 개표관리위원회에 부여한다.
(5) 유권자 명단이 확정되면 투표관리위원회와 개표관리위원회는 전체 유권자 인원에 맞추어 무작위 수열(random sort sequence)을 생성한다. 만약 유권자가 10명일 때 무작위 수열의 예는 5, 6, 4, 8, 9, 0, 2, 3, 1, 7과 같이 서로 겹치는 숫자가 없도록 무작위로 나열한 수열을 뜻한다. 이 수열은 투표관리위원회와 개표관리위원회가 각각 생성하고 외부로 유출되지 않도록 비밀로 유지한다.
(6) 개표관리위원회는 서로 다른 k 종류의 티켓 VN개를 생성한다.

(티켓생성의 예) Ti = 무작위숫자 8자리,
$0 <= i < k$

(7) 개표관리위원회는 VN개의 티켓을 무작위로 섞는다. 예를 들면, k가 5이고 VN이 20일때, T2, T4, T3, T1, T4, T0, T3, T2, T1, T4, T2, T0, T4, T1, T3, T2, T0, T3, T1, T0
(8) 투표관리위원회와 개표관리위원회는 각각 자신의 비밀키와 공개키를 생성하고 이를 이용하여 공인인증기관에게서 인증서를 발급받는다.
(9) 투표관리위원회와 개표관리위원회는 서로의 인증서를 교환한다.

o 투표단계

(1) 투표를 원하는 투표자 Vi는 무작위 숫자(random number) sk2, EC를 생성한다.
(2) 투표자는 투표를 위한 로그인 메시지로 사용하기 위해 다음과 같은 서명값 VC를 생성한다.

$VC = Sign_{Vi\_비밀키}(Hash(EC) \,||\, Ts)$

(3) 투표자 Vi는 투표관리위원회와 개표관리위원회에게 (VC, Ts, Hash(EC), Vi 인증서)를 전송.
(4) 투표관리위원회는 (VC, Ts, Hash(EC), Vi 인증서)를 전송받은 후 서명 값 VC를 검증한다.

$Verify_{Vi\_공개키}(VC, Hash(EC) \,||\, Ts)$

(5) 투표관리위원회는 공인인증기관과 통신하여 Vi의 인증서의 유효성을 검증한다.
(6) 투표관리위원회는 투표자 명단(UserDB)의 EC항목이 기재되어있는지 확인하여, 만약 기재되어있다면 이미 투표한 자라고 알리고 투표를 종료시킨다. (이중 투표 검사)
(7) 아직 투표하지 않은 정당한 투표자임이 확인되면, 투표관리위원회의 공개키가 포함된 공인인증서를 투표자에게 전송한다.
(8) 개표관리위원회도 위 (4)부터 (6)의 과정을 동일하게 수행하여 아직 투표하지 않은 정당한 투표자인지 확인하고 개표관리위원회의 공개키가 포함된 공인인증서를 투표자에게 전송한다.
(9) 투표자는 투표관리위원회, 개표관리위원회의 인증서를 전송받은 후 인증서의 유효성을 검증한다.
(10) 개표관리위원회는 무작위 숫자(random number) sk1를 생성하고, 투표자의 공개키로 암호화하여 전송한다.

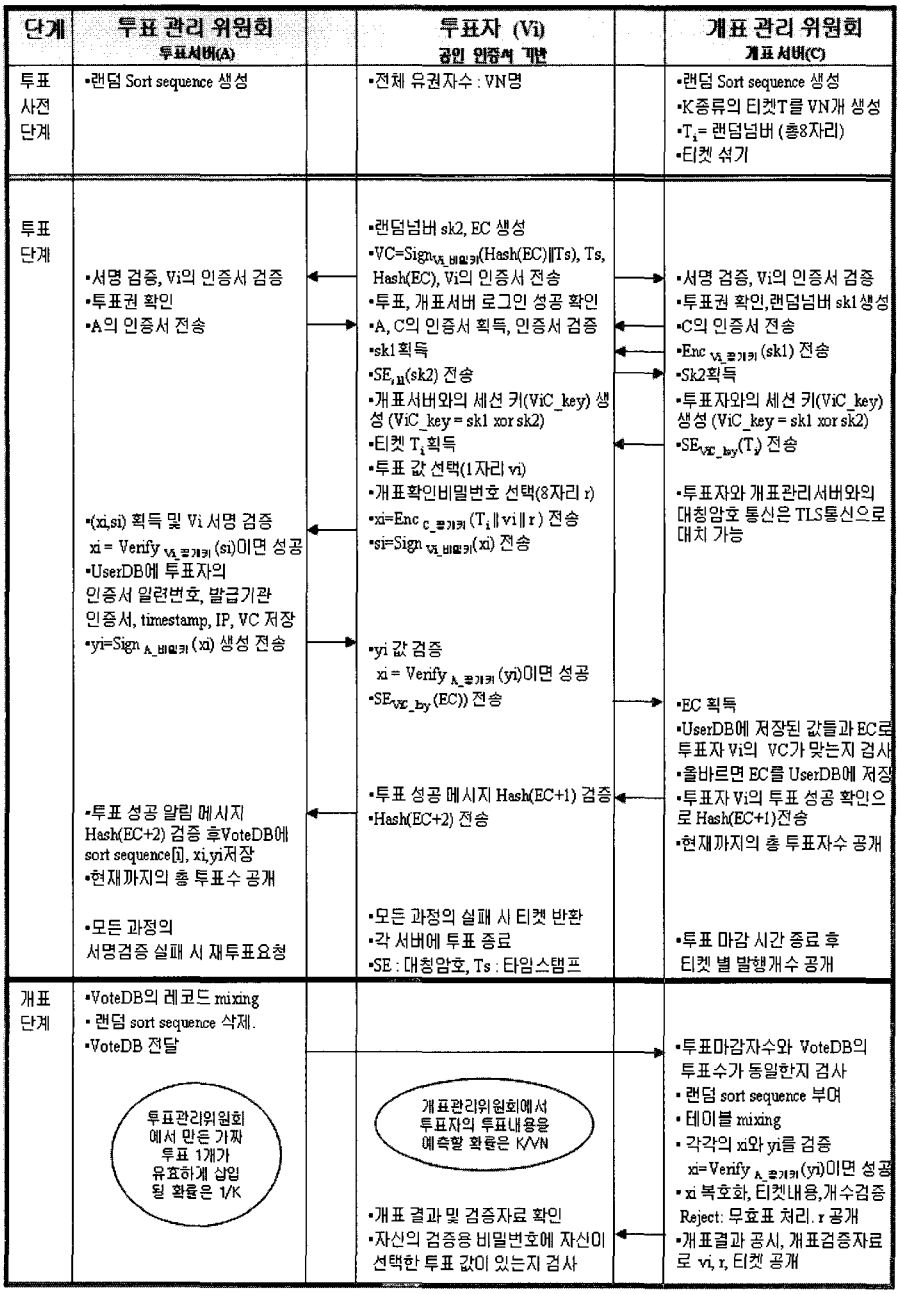
$CSK1 = Enc_{Vi\_공개키}(sk1)$

(11) 투표자는 CSK1을 전송받아, 복호화하여 sk1을 획득한다.

$sk1 = Dec_{Vi\_비밀키}(CSK1)$

(12) 투표자는 자신이 생성했던 sk2를 sk1으로 대칭키 암호알고리즘으로 암호화하여 CSK2를 생성하고 이를 개표관리위원회에게 전송한다.

$CSK2 = SE_{sk1}(sk2)$



〔그림 4〕 PKI 환경에서의 전자 투표 프로토콜

(13) 개표관리위원회는 CSK2를 전송받아, sk2를 획득한다.

$sk2 = SE_{sk1}(CSK2)$

(14) 투표자와 개표관리위원회 : 세션키 생성

ViC_key = sk1 xor sk2

(15) 개표관리위원회는 사전단계에서 생성해 놓았던 무작위로 섞어진 티켓 중 순서대로 하나를 뽑아 투표자와의 세션키로 암호화하여 전송한다.

$CT = SE_{ViC\_key}(T)$

(16) 투표자는 개표관리위원회에게서 CT를 받아 이를

세션키로 복호화하여 티켓 T를 획득한다.

(17) 투표자는 투표를 원하는 투표값 v와 개표검증을 위한 8자리 비밀번호 r을 선택한다.

(18) 투표자는 개표관리위원회의 공개키로 암호화된 투표값 xi를 만든다.

$xi = Enc\ C\_공개키(T \mid\mid v \mid\mid r)$

(19) 투표자는 xi를 투표자의 비밀키로 서명하여 si를 만든다.

$si = Sign_{Vi\_비밀키}(xi)$

(20) 투표자는 xi, si를 투표관리위원회에게 전송.

(21) 투표관리위원회는 xi, si를 획득하여 si의 서명을 검증한다.

$Verify_{Vi\_공개키}(si, xi)$

(22) 서명 검증이 성공하면 UserDB에 투표자 Vi의 인증서 일련번호, 인증서 발급기관, 인증서, Ts, 인터넷 주소(IP), VC를 저장한다.

(23) 투표관리위원회는 xi를 자신의 비밀키로 서명하여 yi를 생성하여 투표자에게 전송한다.

$yi = Sign_{A\_비밀키}(xi)$

(24) 투표자는 투표관리위원회에게서 yi를 받아 서명 검증한다.

$Verify_{A\_공개키}(yi, xi)$

(25) yi에 대한 서명검증이 성공하면, 자신의 투표가 올바르게 투표함에 전송되어 투표가 완료되었다는 의미로 EC를 개표관리위원회와의 세션키로 암호화하여 개표관리위원회에게 전송한다.

$CEC = SE_{ViC\_key}(EC)$

(26) 개표관리위원회는 투표자에게서 CEC를 전송받아 세션 키 ViC_Key로 복호화하여 EC를 획득한다.

$EC = SE_{ViC\_key}(CEC)$

(27) 개표관리위원회는 UserDB에 저장된 값들과 투표자에게서 전송받은 EC를 이용해 최초에 전송받았던 VC가 만들어지는지 검증함으로써 올바른 EC가 전송되었는지, 투표관리위원회에서 UserDB에 관련값들을 올바르게 기록하였는지 검사한다.

(28) 올바르게 검증이 이뤄졌다면 투표자의 투표가 올바르게 성공하였다는 확인으로 Hash(EC+1)를 투표자에게 전송하고, EC값을 UserDB에 기록.

(29) 투표자는 Hash(EC+1)를 전송받아 자신의 EC에 맞는 값인지 검사하고, 올바르면 투표가 성공적으로 종료됨에 동의한다는 의미로 Hash(EC+2)를 투표관리위원회에게 전송한다.

(30) 투표관리위원회는 Hash(EC+2)를 받아 UserDB에 기록된 EC에 올바른 값인지 검증한다.

(31) 검증 성공 시, 투표가 올바르게 종료되었음을 투표자에게 알리고, 투표함 VoteDB에 투표 사전 단계 (5)에서 만든 random sort sequence[i]와 xi, yi를 저장한다.

(32) 투표관리위원회와 개표관리위원회는 현재까지의 총 투표자수를 공개게시판을 이용해 공개한다.

(33) 투표과정 중 각 위원회에서 검증작업이 실패할 경우 재투표를 요청하며, 투표자는 티켓을 개표관리위원회에게 반환하고 투표단계의 1번부터 재시작.

(34) 또 다른 투표자가 투표를 요청할 경우 투표단계의 1번부터 다시 시작한다.

(35) 투표자와 개표관리위원회간의 대칭암호통신은 TLS 통신 등으로 대체가능하다.

o 개표단계

(1) 투표 시간이 종료된 후 개표관리위원회는 티켓 종류별 발행 개수를 공개한다.

(2) 투표관리위원회는 투표 종료 후 부여된 랜덤 수열에 의해 투표함의 xi, yi 쌍을 정렬한다. (Sort)

(3) 투표관리위원회 VoteDB에 기재된 Number를 지우고 개표관리위원회에게 전달한다.

(4) 개표관리위원회는 투표함을 받아 사전단계 (5)에서 생성했던 서로 다른 수로 이루어진 무작위 수열을 xi, yi 쌍에 부여한다.

(5) 개표관리위원회는 위에서 부여된 랜덤 수열에 의해 투표함의 xi, yi 쌍을 정렬한다. (Sort)

(6) 개표관리위원회는 VoteDB에 기재된 Number를 지우고 투표함을 공개하고 개표한다.

(7) 개표관리위원회는 투표 마감자수와 VoteDB의 투표수가 일치하는지 검사한다.

(8) 개표관리위원회는 각각의 xi, yi쌍에 대하여 투표관리위원회의 공개키로 yi의 서명을 검증한다.

$Verify_{A\_공개키}(yi,xi)$

(9) 개표관리위원회는 xi를 자신의 비밀키로 복호하하여 투표내용과 티켓, 개표검증비밀번호 획득.

$(T \mid\mid v \mid\mid r) = Dec_{C\_비밀키}(xi)$

(10) 개표관리위원회는 티켓 발행내역과 검증하여 올바른 티켓이 포함되었는지, 그 개수는 발행현황과 일

치하는지 검사하고 투표내용을 집계한다.

(11) 개표관리위원회는 개표결과를 집계하여 발표하고, 개표검증자료로 r, v, T를 공개한다.

(12) 투표자들은 개표 검증 자료 중에서 자신이 골랐던 r이 있는지 찾고 그것에 대응되는 v값이 자신이 선택한 투표내용인지 검사하여 자신의 투표값이 정확히 개표결과에 반영되었는지 확인할 수 있다. 또한 투표자는 전체 투표자수와 개표결과 발표된 총 집계 결과가 일치하는지, 티켓 발행 현황은 일치하는지 검사하여 투표관리위원회와 개표관리위원회의 부정여부를 검사할 수 있다.

(13) 이러한 과정을 통해 투표관리위원회에서 만든 가짜 투표 1개가 유효하게 삽입될 확률은 1/k이 되며, 개표관리위원회에서 특정 투표자의 투표내용을 예측할 확률은 k/VN이 된다.

Ⅵ. 안전성 및 효율성 분석

1. 안전성 분석

1.1 완전성 (Completeness / Perfection)

투표자의 투표가 완료되면 양 서버가 총 투표자수를 각각 발표하므로 한쪽이 정당한 투표를 삭제했을 경우 서로 총 투표자 수가 불일치하게 된다. 개표결과 검증 시 투표자는 자신이 선택한 개표 확인 검증번호로 자신의 투표 내용의 개표 사실을 확인할 수 있으므로 서버는 정당한 투표를 삭제 할 수 없다.

1.2 건전성 (Soundness)

투표서버는 개표서버에서 총 투표자수를 공개하므로 정당한 투표를 삭제하고 부정투표를 삽입해야 한다. 그러나, 삭제할 정당한 투표의 티켓이 어떤 것인지 알 수 없으므로, 티켓종류를 맞춰 부정투표를 삽입할 확률은 개당 1/k이 된다. 만약 n개의 부정 투표를 삽입하려면 (1/k)n의 확률로 성공가능하며, 이는 그런 행위의 위험성에 비해 매우 희박한 확률이다.

1.3 기밀성, 익명성 (Privacy)

개표 직전 xi, yi가 공개되고, 개표 후 xi가 복호화 된 뒤 투표내용과 개표확인 비밀번호, 티켓종류가 공개된다. 개표서버는 티켓 종류별로 어떤 투표자에게 발행했는지 알 수 있지만, 같은 종류의 티켓을 부여받은 투표자는 VN/k이다. 그러므로 이러한 정보를 토대로 투표자의 투표내용을 예측할 확률은 k/VN으로 찬반투표의 경우 한 투표자의 투표 내용을 맞출 확률인 (1/2)보다 작다. 유권자의 수와 과거 선거의 투표율, 후보자의 수등을 고려하여 티켓의 종류 k를 적절하게 조절한다면 특정 투표자의 투표내용을 예측할 확률을 낮게 조절할 수 있다.

1.4 이중 투표 불가성 (Unreusability)

VC=Sig $_{Vi\_비밀키}$(Hash(EC)||Ts)에 포함되어있는 적합한 EC를 생성할 수 있는 사람은 투표자밖에 없다. 올바른 과정에 의해 투표를 마쳤을 경우 투표자는 EC를 공개하여야 하고, VC에 맞는 EC가 유권자 명단에 기록되어야만 투표함에 투표가 저장되고 투표 완료한 것으로 인정된다. 만약 차후에 자신의 투표를 부인할 경우에는 VC와 EC, 투표자의 인증서를 이용해 검증해 볼 수 있고 VC에 맞는 EC가 기록되어있다면, VC생성에 투표자가 자신의 비밀키를 사용했다는 증거이므로 투표가 올바르게 종료된 것임을 선관위는 주장할 수 있다.

1.5 적임성 또는 투표권 (Eligibility)

양 서버는 인증기관과 함께 투표를 위한 접속자의 신분(실명)과 올바른 유권자의 인증서인지를 검사하고, 유권자 명단의 투표권 여부와 투표 실시 여부를 검사하므로 투표권이 없는 투표자는 투표할 수 없다. 이러한 방식의 부정 투표는 선거관리위원회에서 유권자 명단을 허위로 작성해야만 가능하다.

1.6 공정성 (Fairness)

투표 내용은 검증확인용 비밀번호, 티켓과 함께 개표서버의 공개키로 암호화되므로 개표서버의 비밀키 없이는 투표 내용을 알 수 없다. 개표서버는 투표 종료 전까지 투표함 접근이 불가능하므로 투표내용 추적 불가능.

1.7 검증성 (Verifiability)

o 전체 검증성 : 투표함에 담긴 투표 수와 각 서버에서 발표되는 투표자 수, 개표 서버의 티켓 발행 개수가 일치하는지 검사하여 부정 투표가 삽입되는지 검사. 투표서버의 인증서, 개표서버의 인증서, 개표에 사용된 xi, yi가 공개되므로, 개표 내용(투표값, 비밀번호, 티켓)에 대한 올바른 암호값 xi인지, 투표서버의 서명 yi가 맞는지 검사. 개표 집계 결과와 위에서 검증된 투표 내용별 개수 집계가 맞는지 검사.

o 개별 검증성 : 투표자는 자신이 선택한 개표 확인비밀번호에 해당되는 투표 내용이 자신이 선택한 투표내용

인지 검사.

1.8 매표 불가능성 (no tradablility)

매표 불가능성이란 결국 자신의 투표내용을 타인이 검사할 수 없어야만 가능하다. 이는 위에서 언급한 검증성, 특히 개별 검증성과는 반대되는 성격으로 서로 Trade-off 관계에 있다. 본 논문에서 제시한 시스템에서는 개별 검증성을 만족하기 위해 개표 확인 비밀번호를 사용했다. 그러므로 매표행위를 막을 수는 없다. 투표자 개인이 선택한 개표 확인용 비밀번호를 이용해 개표 결과에 대한 개별 검증이 가능하므로, 매수자는 투표자의 투표내용과 개표확인용 비밀번호를 밝히도록 하여 투표자의 투표 사실을 확인할 수 있다. 하지만, 만약 선거의 규모와 중요도, 여론등을 감안하여 개별 검증성을 포기하고 매표행위를 막는다면, 개표확인 비밀번호를 개표 후 발표하지 않으면 된다. 결국, 현재 제안된 시스템은 개표 결과 검증 자료로 투표 내용을 공개하고, 이를 바탕으로 개별 검증성을 갖추고 있기 때문에 매표행위를 방지할 수 있는 기능은 없으나, 매표 행위를 방지하고 개별 검증성을 포기하길 원한다면, 개표 집계 후 개표 확인 비밀번호를 공개하지 않음으로써 매표 행위를 방지 할 수 있다.

2. 효율성 분석

본 논문에서 제안하는 전자 투표 프로토콜은 다른 전자 투표 프로토콜보다 서비스 현실에 중점을 두어 새로운 개념의 안전성을 요구하고 있고 이들을 만족하기 위해 프로토콜이 꾸며져 있다. k종류의 티켓이라는 장치를 활용해서 투표서버의 부정투표를 차단한 부분이나 EC값과 관련한 해쉬값을 전달해주면서 투표자의 부인봉쇄 기능을 첨가한 부분들은 다른 전자 투표 프로토콜에는 도입되지 않은 장치들이다. 그러므로 다른 전자 투표 프로토콜과 연산량 횟수를 비교하기 위해 이러한 부가적인 장치들은 제외하기로 했다. 다음 표는 암호화와 서명기법으로 RSA를 사용했을때 "An Improvement on a Practical Secret Voting Scheme"와 본 논문에서 제안하는 전자투표 프로토콜이 갖는 지수승 연산 횟수를 비교해서 나타낸 표이다. "An Improvement on a Practical Secret Voting Scheme"은 투표자와 투표내용에 대한 연계정보를 감추기 위해 Mix 서버를 따로 두고 있다. 이는 메시지 전송 횟수와 암복호화 횟수를 더 증가시키는 요인이 되기도 한다. 이러한 단점을 개선하여 은닉암호 생성을 간단히 수행하도록 하고, Mix 서버의 기능을 투표 서버와 개표 서버에게 분배한 결과 연산량이 감소되었음을 볼 수 있다.

연산량 측면에서의 효율성뿐만 아니라, 본 시스템은 기존의 PKI 환경을 그대로 사용하면서 구현할 수 있도록 디자인되어있고, Mix 서버를 따로 두지 않고 있기 때문에 여러 가지 면에서 수치로 표현하기는 어려운 효율성을 가지고 있다. 또 특정 암호 알고리즘에 의존하지 않고 있으므로 시스템 구축에 대한 제한이 없으며, 환경에 따라 적절한 공개키 암호 알고리즘을 적용한다면, 모바일에서도 본 시스템을 구현하여 운영할 수 있을 것이다.

Ⅶ. 서비스 현실화를 위한 부가사항

인터넷 전자 투표 시스템을 현실화하여 실제 대규모 서비스하기 위해서는 본 논문에서 제안된 시스템에 부가적으로 각종 환경적, 정책적인 문제들이 선행되어야 한다. 다수의 투표자가 동시에 접속하여 투표를 하려면 많은 연산을 원활히 수행하고, 빠른 개표를 문제없이 처리할 수 있도록 분산 연산이 가능한 서버 측 환경이 마련되어야 한다. 또, 특정 짧은 시간에 많은 투표자들이 접속할 수 있으므로 네트워크 트래픽 관리도 매우 중요한 사항이다. 혹시라도 서버가 다운되는 현상이 일어나더라도 즉각적으로 예비 서버가 가동되도록 하는 시스템 이중화가 필요하며, 투표함, 유권자 등록 정보 등 중요한 데이터베이스에 대한 백업 및 보안 관리도 필수적이다. 특히, 데이터베이스 보존 및 백업, 각종 로그 데이터 관리문제는 체계적으로 이루어질 수 있게 법제화할 필요가 있다.

〔표 1〕 연산량 효율성 비교

구 분	An Improvement on a Practical Secret Voting Scheme[3]			제안하는 전자 투표 프로토콜		
	암복호화	서명/검증	은닉서명	암복호화	서명/검증	은닉서명
등록단계	1	3	1	-	-	-
투표단계	2	2	-	1	7	-
개표단계	3	3	-	1	1	-
총계	6	8	1	2	8	-

이를 통해 차후에 악의적으로 이용할 수 없도록 해야 한다. 이러한 여러 가지 제반 사항이 완벽히 갖추어진 상태에서 실제 서비스가 가능할 것이다. 전자선거라는 특수한 상황은 세계 수많은 해커와 정보전 요원들의 공격 대상이 될 것이므로 네트워크 및 데이터베이스에 대한 공격은 충분히 예상될 수 있는 문제이며, 문제가 발생할 경우 커다란 혼란을 불러올 수도 있기 때문이다.

Ⅷ. 결 론

"전자정부 로드맵"에 따르면 참여민주주의의 실현을 위해 전자투표제, 전자선거제를 시범 도입하여, 정부의 정책에 국민들이 쉽게 참여할 수 있도록 할 계획이라고 한다. 참다운 직접민주주의 상징으로 알려진 아크로폴리스 광장이 이제는 인터넷을 통해 사이버공간에서 재현될 수도 있을 것이다. 본 논문에서는 은닉 서명과 공개키 암호에 기반한 기존 전자투표 프로토콜을 보다 효율적이고 안전하게 개선하였다. 제안된 시스템은 특정 암호 알고리즘에 국한되지 않아 여러 가지 환경에 맞게 더 효율적으로 응용하여 구현할 수 있을 것이다. 투표함의 내용을 섞어 투표자와 투표내용을 연관시켜 유추할 수 없도록 하는 믹스 서버의 기능을 개표서버와 투표서버와 개표서버에 분산시킴으로서 암호화와 복호화의 연산량을 줄였고, 공인인증서를 활용 할 수 없을 경우에도 시스템의 큰 변경없이 패스워드 인증 방식을 사용 할 수 있다. 특히, 유권자의 수와 과거 투표율, 후보자수에 맞춰 티켓의 종류 개수를 조절함으로써 투표자의 익명성을 유지하면서 투표서버의 부정 표 삽입을 차단하는 기능을 고안했다. 전자투표가 현실화되기 위한 가장 중요한 요소인 투표 서버와 개표서버의 신뢰성을 높이기 위해 노력하였다.

참 고 문 헌

[1] 허원근, 김희선, 김광조, "전자선거 프로토콜의 요구사항 연구"

[2] A. Fujioka, T. Okamoto and K. Ohta, "A Practical Secret Voting Scheme for Large Scale Election", *Advances in Cryptology-Auscrypt'92, LNCS Vol.718*, pp.248-259, Springer-Verlag, 1993.

[3] M. Ohkubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto, "An Improvement on a Practical Secret Voting Scheme", *Information Security'99, LNCS Vol.1729*, pp.225-234, Springer-Verlag, 1999.

[4] A. Fujioka, M. Abe, M. Ohkubo, and F. Hoshino, "An Implementation and an Experiment of a Practical and Secure Voting Scheme", *Proc. of SCIS2000, C48, Okinawa, Japan*, Jan. 26-28, 2000.

[5] 김광조, "Killer Application of PKI to Internet Voting"

[6] 김진호, 김광조, "공개키 기반 구조 하에서의 안전한 인터넷 전자투표 프로토콜 설계"

[7] J. Camenisch, J. Pireteau, and M. Stadler, "Blind Signatures based on the Discrete Logarithm Problem", *Advances in Cryptology-EUROCRYPT'94, LNCS Vol. 950*, pp428-432 Springer-Verlag, 1994.

[8] Ivan Damagard, Mads Jurik, "Client/Server Tradeoffs for Online Elections", *PKCS2002, LNCS 2274*, pp.125-140, 2002.

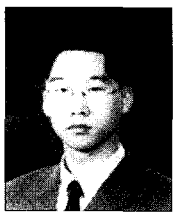
[9] C. Andrew Neff, Jim Adler, "Verifiable e-Voting", VoteHere, Inc

[10] 김재광, "전자투표의 도입에 따른 관련법제 정비 방안", 한국법제연구원

[11] 김재광, "인터넷투표의 도입에 따른 문제점과 개선방안", *전자투표와 관련한 법적 과제*, 한국법제연구원, 2002. 3

[12] 박동진, "전자 투표 도입의 전제조건", 고려대학교 아세아 문제 연구소

〈著 者 紹 介〉



이 래 (Rae Lee)
정회원

2002년 2월 : 고려대학교 전산학 학사
2004년 2월 : 고려대학교 정보보호대학원 공학석사
2004년 6월~현재 : 국가보안기술연구소(NSRI) 연구원
〈관심분야〉 정보보호, 암호응용, 프로토콜, 컴퓨터 알고리즘, 전자정부

이 동 훈 (Dong Hoon Lee)
종신회원

1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
〈관심분야〉 정보보호, 암호이론, 프로토콜, 정보이론